Semi-device independent random number expansion protocol with $n \to 1$ quantum random access codes

Hong-Wei Li,[1] Marcin Pawłowski,[2] Zhen-Qiang Yin,[1] Guang-Can Guo,[1] and Zheng-Fu Han[1]
[1]*Key Laboratory of Quantum Information,University of Science and Technology of China,Hefei, 230026, China*
[2] *Department of Mathematics, University of Bristol, Bristol BS8 1TW,United Kingdom*
(Dated: March 6, 2012)

We study random number expansion protocols based on the $n \to 1$ quantum random access codes (QRACs). We consider them in the semi-device independent scenario where the inner workings of the devices are unknown to us but we can certify the dimensions of the systems being communicated. This approach does not require the use of the entanglement and makes the physical realization of these protocols much easier than in the standard device independent scenario. In our work, we propose a protocol for randomness expansion, compute min-entropy for the semi-device independent protocol, and investigate $n \to 1$ QRACs with a view to their use in randomness expansion protocols. We also calculate the dependence of the effectiveness of the randomness generation on n and find it optimal for $n = 3$, and provide the explanation for this fact.

arXiv:1109.5259v2 [quant-ph] 13 Mar 2012

Introduction - To certify that the given set of random numbers is truly random is not an easy task. Since these numbers cannot be generated by the deterministic algorithms, the devices that generate them must operate according to some intrinsically random physical process. The problem reduces then to the certification that the device really performs the way it is supposed to, at least within reasonable limits. The device independent approach [1] allows the parties to establish the parameters necessary for this certification without having to physically examine the details of the device. This approach has been highly successful in the quantum cryptography [2–4] and recently has been taken to study also the randomness generation. Colbeck [5, 6] has proposed the true random number expansion protocol based on the GHZ test and Pironio *et al.* [7] have proposed the protocol based on the Bell inequality violations. All these protocols require entanglement which has the negative effect on the complexity of the devices and the rates of the randomness generation [7].

The notion of semi-device independent, which assumes the knowledge of the dimension of the underlying physical system but otherwise nothing about the actual physical implementation of the measurements, was first introduced by Liang *et al.* [8] in the context of bounding entanglement. Working within the same framework, a compromise between the need to know the devices and the requirement for quantum resources was proposed [9]. In this scenario, secure key distribution without entanglement has been proposed. More recently, the same approach has also been used to certify true randomness [10].

In both papers [9, 10] the parameter estimated to certify the devices was the average success probability of the $2 \to 1$ Quantum Random Access Code (QRAC). This protocol has been firstly proposed in [11] allows one party, the sender, to encode two classical bits in one qubit in such a way that the second party which receives this qubit can decode any one of the two classical bits with the success probability strictly greater than $\frac{1}{2}$. Generalizations of it to $n \to 1$ QRACs, i.e. the protocols where n classical bits are encoded in a single qubit, have then been proposed and studied [12–15]. Here we generalize the results from [10] and study the true random number generation protocols based on $n \to 1$ QRACs. We are particulary interested in the amount of randomness generated as a function of n. We find that, remarkably, this function is not monotonic and reaches the maximum for $n = 3$. We provide the explanation of this fact.

The paper is structured as follows. First we describe the semi-device independent scenario. Then we show how it can be used for the randomness generation. Later we calculate the amount of randomness generated as the function of n and present in more detail the protocol that generates most randomness. We end with the discussion of our results.

Semi-device independent scenario - The semi-device independent random number generation [22] protocol requires two black boxes, which are used for the state preparation and measurement respectively.

1. State preparation black box: The preparation box is given randomly one of the 2^n inputs a represented by n different bits $a = a_1 \cdots a_n$. For each input this box emits the state ρ_a which is sent to the measuring box.

2. State measurement black box: There one of n different measurements $y = \{1, \cdots, n\}$, is chosen and the outcome $b = \{0, 1\}$ returned.

3. QRAC average success probability estimation: Applying random input numbers a, y and measurement outcomes b to estimate QRAC average success probability, which can be used for guarantee randomness of the measurement outcomes.

4. Random number generation: The parameter that is used to the randomness of the measurement outcome b conditioned on the input values a and y is the min-entropy function (It's used for extractors both

in classical and quantum cases) [16, 17] given by

$$H_\infty(B|A,Y) \equiv -log_2[max_{b,a,y}P(b|a,y)]. \qquad (1)$$

Since it is the semi-device independent scenario we do not have any knowledge of the measurements and the preparations apart from the fact that for all a the states ρ_a are of dimension 2, and they are not parts of any lager entangled systems. This scenario is schematically depicted on FIG. 1.

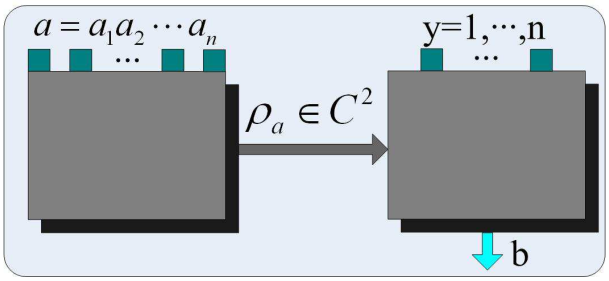

FIG. 1: Semi-device independent random number expansion protocol.

Certification parameters - The certification of the device requires the estimation of the probabilities

$$P(b|ay) = tr(\rho_a M_y^b), \qquad (2)$$

where, M_y^b is the measurement operator acting on the two dimensional Hilbert space with the input parameter y and the output parameter b. The advantage of the semi-device independent approach is that these probabilities are the only numbers that need to be calculated in order to find the parameter that certifies the device. This parameter is, as we have mentioned, the average success probability of the $n \to 1$ QRAC given by

$$S_n \equiv \frac{1}{n2^n}\sum_{a,y} P(b = a_y|a,y), \qquad (3)$$

but for our purposes it will be more convenient to use

$$T_n \equiv \Sigma_{a,y}(-1)^{a_y}E_{ay}, \qquad (4)$$

where $E_{ay} = P(b=0|ay)$.

By $T_n^{classical}$ we denote the greatest value of T_n possible if the communicated system is a classical bit. By $T_n^{quantum}$ the same value for qubit. The corresponding values for $n = 2, 3, 4, 5$ are

$$\begin{array}{lll} T_2^{classical} \le \ 2, & T_2^{quantum} \le \ 2.828427, & n=2, \\ T_3^{classical} \le \ 6, & T_3^{quantum} \le \ 6.928203, & n=3, \\ T_4^{classical} \le 12, & T_4^{quantum} \le 15.454813, & n=4, \\ T_5^{classical} \le 30, & T_5^{quantum} \le 34.172467, & n=5. \end{array} \qquad (5)$$

They correspond to the codes presented in [14].

The intuition behind using these codes to generate the randomness is that the more bits are encoded into the single qubit the less certain is the correct guessing of any of them. We find the result that the amount of randomness is not a monotonous function of n remarkable since the parameters S_n and $\frac{T_n^{quantum}}{T_n^{classical}}$ are.

Amount of randomness - The main result of this paper is the amount of the randomness generated by $n \to 1$ QRACs in the semi-device independent scenario.

More precisely, we solve the following optimization problem:

$$\begin{array}{ll} \text{minimize:} & max_{b,a,y}P(b|a,y) \\ \text{subject to:} & E_{ay} = tr(\rho_a M_y^0) \\ & \Sigma_{a,y}(-1)^{a_y}E_{ay} = T_n \end{array} \qquad (6)$$

where the optimization is carried over arbitrary quantum states ρ_a and measurement operators $\{M_1^0, \cdots, M_n^0\}$ defined over 2-dimensional Hilbert space. In the most general case, we should consider the positive operator valued measure (POVM) $\{M_j^0, M_j^1\}$, where $M_j^0 + M_j^1 = I$ for $j \in \{1, \cdots, n\}$. Fortunately, Masanes [18] has proved that only the projective measurements should be considered in the case of 2-measurement outcomes have to be considered(Jordan *et al.* [19, 20] have showed that such binary measurements commute with a projective measurement). Since T is the linear expression of the probabilities, we can only consider pure states [21] in the numerical calculation. Without the loss of generality, the state preparation and measurements in our numerical analysis can be illustrated with the following equations

$$\rho_a = |\varphi(a)\rangle\langle\varphi(a)|, \qquad (7)$$

$$|\varphi(a)\rangle = \begin{pmatrix} cos(\frac{\theta_a}{2}) \\ e^{i\eta_a}sin(\frac{\theta_a}{2}) \end{pmatrix}, \qquad (8)$$

$$M_1^0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad (9)$$

$$M_j^0 = \begin{pmatrix} cos^2(\frac{\psi_j}{2}) & \frac{1}{2}e^{-i\omega_j}sin(\psi_j) \\ \frac{1}{2}e^{i\omega_j}sin(\psi_j) & sin^2(\frac{\psi_j}{2}) \end{pmatrix}, \qquad (10)$$

where $a \in \{\overbrace{\underbrace{00\cdots0}_{n}, \cdots, \underbrace{11\cdots1}_{n}}^{2^n}\}$, $j \in \{\overbrace{2, \cdots, n}^{n-1}\}$, $0 \le \theta_a, \psi_j \le \pi$, $0 \le \eta_a, \omega_j \le 2\pi$.

By solving the minimization problem, we get the min-entropy bound of the measurement outcome for the given $n \to 1$ QRAC. If we set $T_n = T_n^{quantum}$ we get the maximal amount of randomness generated by the given QRAC. We obtain the following results

$$\begin{array}{ll} n=2 & H_\infty \simeq 0.2284 \\ n=3 & H_\infty \simeq 0.3425 \\ n=4 & H_\infty \simeq 0.1388 \\ n=5 & H_\infty \simeq 0.1024 \end{array}$$

Note that the min-entropy bound based on $2 \to 1$ QRAC is larger than our previous result [10], the reason for which is that the maximal quantum correlation value $T_2^{quantum}$ is approximated to six decimal places. Fig. 2 shows that even the small changes of T_2 lead to very large changes in the min-entropy bound if T_2 is close to the maximal quantum value.

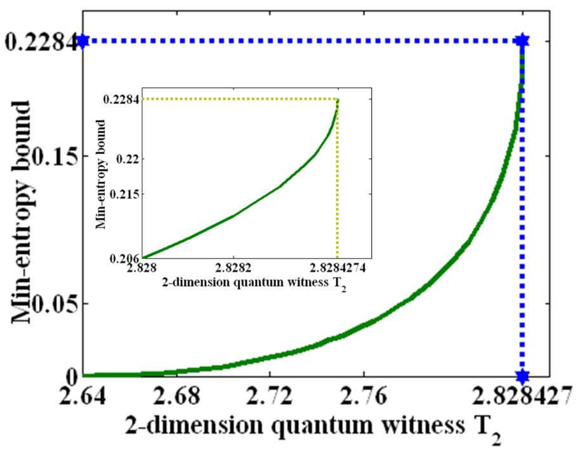

FIG. 2: The relationship between the average efficiency of $2 \to 1$ QRAC measured by T_2 and the min-entropy bound.

As we have already mentioned the largest amount of the randomness is generated with the $3 \to 1$ QRAC. Now we describe in this code more detail.

Randomness generated by $3 \to 1$ **QRAC -** The optimal protocol generates 0.1141 more per the run of the experiment than the first semi-device independent randomness generation protocol introduced in [10]. The lower bound on the amount of randomness generated as the function of T_3 is plotted in Fig. 3. The result show that we can get the positive amount of randomness as soon as $T_3 > 6.65$.

The parameters $T_3^{quantum}$ and $H_\infty = 0.3425$ can be obtained using the following $3 \to 1$ QRAC. The state prepared by the first black box is given by

$$\begin{aligned}
|\varphi(000)\rangle &= cos(\xi)|0\rangle + e^{i\frac{\pi}{4}} sin(\xi)|1\rangle,\\
|\varphi(001)\rangle &= cos(\xi)|0\rangle + e^{-i\frac{\pi}{4}} sin(\xi)|1\rangle,\\
|\varphi(010)\rangle &= cos(\xi)|0\rangle + e^{i\frac{3\pi}{4}} sin(\xi)|1\rangle,\\
|\varphi(011)\rangle &= cos(\xi)|0\rangle + e^{-i\frac{3\pi}{4}} sin(\xi)|1\rangle,\\
|\varphi(100)\rangle &= sin(\xi)|0\rangle + e^{i\frac{\pi}{4}} cos(\xi)|1\rangle,\\
|\varphi(101)\rangle &= sin(\xi)|0\rangle + e^{-i\frac{\pi}{4}} cos(\xi)|1\rangle,\\
|\varphi(110)\rangle &= sin(\xi)|0\rangle + e^{i\frac{3\pi}{4}} cos(\xi)|1\rangle,\\
|\varphi(111)\rangle &= sin(\xi)|0\rangle + e^{-i\frac{3\pi}{4}} cos(\xi)|1\rangle,
\end{aligned} \tag{11}$$

where $\xi = arccos\sqrt{\frac{1}{2} + \frac{\sqrt{3}}{6}}$. For the state measurement in the second black box, we use the three projective measurements with the following bases

$$\begin{aligned}
&\{M_1^0 = |0\rangle\langle 0|, \quad M_1^1 = |1\rangle\langle 1|\},\\
&\{M_2^0 = |0'\rangle\langle 0'|, \quad M_2^1 = |1'\rangle\langle 1'|\},\\
&\{M_3^0 = |0''\rangle\langle 0''|, \quad M_3^1 = |1''\rangle\langle 1''|\},
\end{aligned} \tag{12}$$

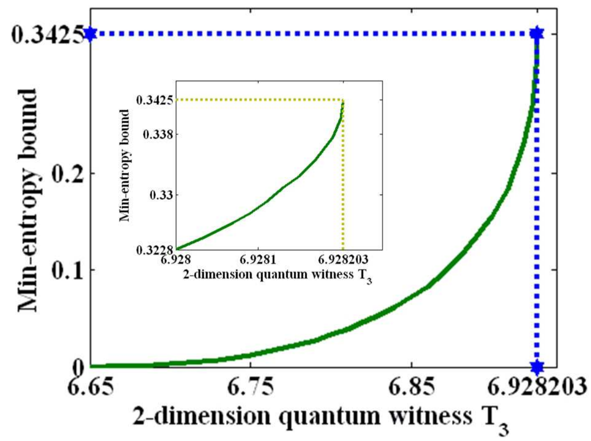

FIG. 3: The relationship between the average efficiency of $3 \to 1$ QRAC measured by T_3 and the min-entropy bound. We see that the positive amount of randomness can be generated as soon as $T_3 > 6.65$, and the maximal value of the min-entropy is 0.3425 with $T_3 = 6.928203$.

where $|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1'\rangle = -\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, $|0''\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |1''\rangle = -\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$.

Discussion - We have presented the family of randomness generation protocols based on the $n \to 1$ QRACs. The certification that the device indeed produces truly random numbers is done in the semi-device independent scenario, which combines the advantages of the standard device independent approach with less requirements on the resources required. We have found that the optimal member of the family, in the sense of the amount of the randomness generated, is the $3 \to 1$ QRAC.

The remarkable feature of this family of codes is that the amount of the randomness as a function of n is not monotonic. To understand why it is so, consider the Bloch sphere. Both the states and the measurements can be represented by the unit vectors on it. If one looks at the constructions for the QRACs from [14] one notices that the states are almost evenly spread on the whole surface of the sphere. Therefore, as n grows, for any measurement the nearest state gets closer and closer. This however does not happen for the transition from $n = 2$ to $n = 3$. The reason for this is that the states and the measurements for the optimal QRAC lie in one plane and do not use the full size of the space.

The $3 \to 1$ QRAC is the most efficient semi-device independent randomness generation protocol known. It remains the open question if even better protocols exist.

In comparison to fully device-independent random number expansion protocols, the protocols presented here are much easier to realize, which makes them a good object for future studies, and one of the most important aspects of it should be the full security proof.

Acknowledgements - H-W. L. thanks Y-C. W., X-B. Z. and Y. Y. for helpful discussions. H-W.L., Z-Q.Y.,

G-C.G. and Z-F.H. are supported by the National Basic Research Program of China (Grants No. 2011CBA00200 and No. 2011CB921200), National Natural Science Foundation of China (Grant NO. 60921091), and National High Technology Research and Development Program of China (863 program) (Grant No. 2009AA01A349) . M.P. is supported by UK EPSRC. To whom correspondence should be addressed, Email: [a]maymp@bristol.ac.uk, [b]zfhan@ustc.edu.cn.

[1] D. Mayers, A. Yao, *FOCS '98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, p.503 Washington DC, USA, (1998).
[2] J. Barrett, L. Hardy, A. Kent, Phys. Rev. Lett. **95**, 010503, (2005).
[3] E. Hänggi, R. Renner, arXiv/1009.1833, (2010). E. Hänggi, R. Renner, S. Wolf, EUROCRYPT 2010, pp. 216-234, (2010).
[4] Ll. Masanes, S. Pironio, A. Acin, Nat. Commun. **2**, 238, (2011).
[5] R. Colbeck, A. Kent, Journal of Physics A: Mathematical and Theoretical, **44(9)**, 095305, (2011).
[6] R. Colbeck, *Quantum and relativistic prtocols for secure multi-party computation*, PHD Thesis, arXiv: 0911.3814, (2009).
[7] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, Nature **464**, 1021, (2010).
[8] Y.-C. Liang, T. Vértesi, N. Brunner, Phys. Rev. A **83**, 022108, (2011).
[9] M. Pawłowski, N. Brunner, Phys. Rev. A **84**, 010302(R), (2011).
[10] H-W Li, Z-Q Yin, Y-C Wu, X-B Zou, S. Wang, W. Chen, G-C Guo, Z-F Han, Phys. Rev. A **84**, 034301, (2011).
[11] S. Wiesner, SIGACT News **15(1)**, 78, (1983).
[12] A. Ambainis, A. Nayak, A. Ta-Shma, U. Vazirani, Journal of the ACM, **49(4)**, 496, (2002).
[13] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond and S. Yamashita, N. J. Phys. **8**, 129, (2006).
[14] A. Ambainis, D. Leung, L. Mancinska, M. Ozols, arXiv:0810.2937, (2008).
[15] M. Pawłowski, M. Żukowski, Phys. Rev. A **81**, 042326, (2010).
[16] R. Koenig, R. Renner, C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337, (2009).
[17] A. De, C. Portmann, T. Vidick, R. Renner , arXiv/0912.5514 , (2009).
[18] L. Masanes, arXiv/0512100, (2005),
[19] C. Jordan, Bulletindela S. M. F. , 3, 103 (1875), B. S. Tsirelson, Hadronic Journal Supplement, 8, 329 (1993).
[20] E. Hänggi, M. Tomamichel, arXiv/1108.5349, (2011).
[21] R. Gallego, N. Brunner, C. Hadley, A. Acin, Phys. Rev. Lett. **105**, 230501, (2010).
[22] Since the protocol in both device independent and semi-device independent cases require some randomness for the certification procedure they are in fact randomness expansion rather than generation protocols.